

*The following security alert was issued by the Information Security Division of the Mississippi Department of ITS and is intended for State government entities. The information may or may not be applicable to the general public and accordingly, the State does not warrant its use for any specific purposes.*

**DATE(S) ISSUED:**

08/14/2012

**SUBJECT:**

Cumulative Security Update for Internet Explorer (MS12-052)

**OVERVIEW:**

Multiple vulnerabilities have been discovered in Microsoft's web browser, Internet Explorer, which could allow an attacker to take complete control of an affected system. Successful exploitation of these vulnerabilities could result in an attacker gaining the same privileges as the logged on user. Depending on the privileges associated with the user, an attacker could then install programs; view, change, or delete data; or create new accounts with full user rights.

**SYSTEMS AFFECTED:**

- Internet Explorer 6
- Internet Explorer 7
- Internet Explorer 8
- Internet Explorer 9

**RISK:**

**Government:**

- Large and medium government entities: **High**
- Small government entities: **High**

**Businesses:**

- Large and medium business entities: **High**
- Small business entities: **High**

**Home users: High**

**DESCRIPTION:**

Four remote code execution vulnerabilities have been reported in Internet Explorer. These vulnerabilities occur due to the way Internet Explorer accesses objects in memory that have not been properly deleted, or initialized. The four vulnerabilities are:

- Layout Memory Corruption Vulnerability - CVE-2012-1526
- Asynchronous NULL Object Access Remote Code Execution Vulnerability - CVE-2012-2521
- Virtual Function Table Corruption Remote Code Execution Vulnerability - CVE-2012-2522
- JavaScript Integer Overflow Remote Code Execution Vulnerability - CVE-2012-2523. This is also addressed in MS12-056.

These may be exploited if a user visits a web page that is specifically crafted to take advantage of the vulnerabilities. Successful exploitation of these vulnerabilities could result in an attacker gaining the same

privileges as the logged on user. Depending on the privileges associated with the user, an attacker could then install programs; view, change, or delete data; or create new accounts with full user rights.

**RECOMMENDATIONS:**

The following actions should be taken:

- Apply appropriate patches provided by Microsoft to vulnerable systems immediately after appropriate testing.
- Run all software as a non-privileged user (one without administrative privileges) to diminish the effects of a successful attack.
- Remind users not to visit un-trusted websites or follow links provided by unknown or un-trusted sources.
- Inform and educate users regarding the threats posed by hypertext links contained in emails or attachments especially from un-trusted sources.

**REFERENCES:****Microsoft:**

<http://technet.microsoft.com/en-us/security/bulletin/ms12-052>